

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-160117

(43)Date of publication of application : 12.06.2001

(51)Int.Cl.

G06K 17/00  
G03G 21/04  
G06F 12/14  
G06K 19/07  
G06K 19/10  
H01Q 1/12  
H04B 5/02  
H04L 9/32

(21)Application number : 11-345330

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 03.12.1999

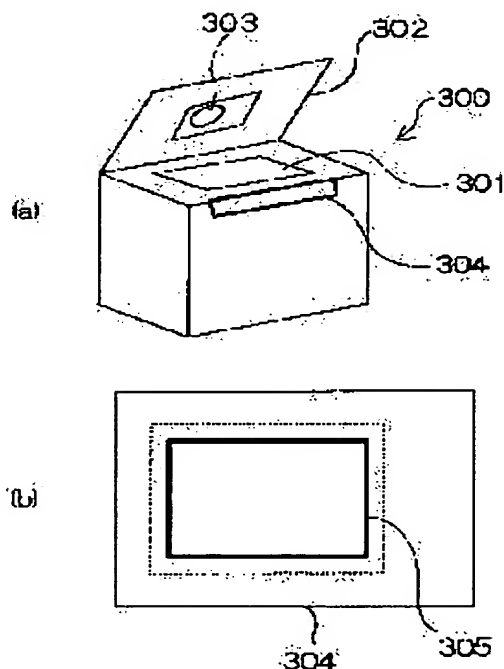
(72)Inventor : ODA YASUNORI

## (54) SYSTEM FOR MANAGING DEVICE SECURITY

(57)Abstract:

PROBLEM TO BE SOLVED: To enable a scrupulous control about the operation of a device needing security management such as copying a confidential document.

SOLUTION: A user is made to carry a RFID and a RFID is also attached to the confidential document. A copying machine 300 is provided with a reader/ writer 303 to read the FRID of the document set in the platen and the FRID of the user in front of the machine 300. The machine 300 is controlled so as to be able to copy the document only when the access right of the user read from the FRID of the user is higher than the confidential level of the document read the FRID of the document on the platen.



## LEGAL STATUS

[Date of request for examination]

20.05.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-160117

(P2001-160117A)

(43)公開日 平成13年6月12日(2001.6.12)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト*(参考)
G 0 6 K 17/00		G 0 6 K 17/00	F 2 H 0 2 7
			L 2 H 0 3 4
G 0 3 G 21/04		G 0 6 F 12/14	3 1 0 K 5 B 0 1 7
G 0 6 F 12/14	3 1 0		3 2 0 C 5 B 0 3 5
	3 2 0	H 0 1 Q 1/12	Z 5 B 0 5 8
審査請求 未請求 請求項の数10 OL (全 12 頁) 最終頁に続く			

(21)出願番号 特願平11-345330

(22)出願日 平成11年12月3日(1999.12.3)

(71)出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72)発明者 黄田 保彦

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

(74)代理人 100075258

弁理士 吉田 研二 (外2名)

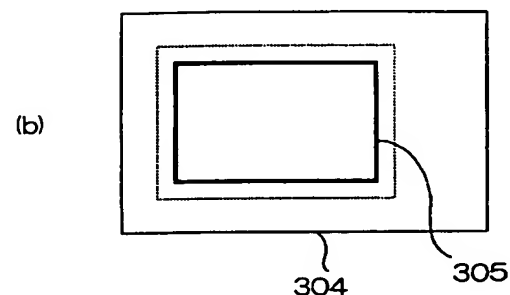
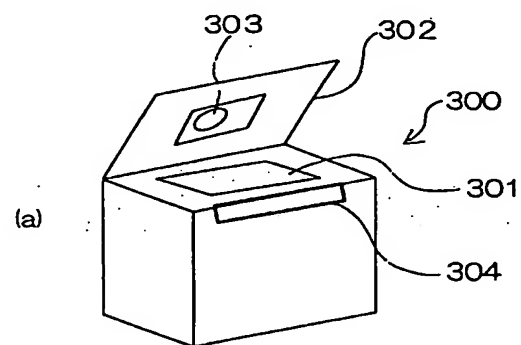
最終頁に続く

(54)【発明の名称】 装置セキュリティ管理システム

(57)【要約】

【課題】 機密文書の複写など、セキュリティの管理を要する装置の動作について、きめ細かい制御を可能にする。

【解決手段】 ユーザにRFIDを携帯させると共に、機密文書にもRFIDを付ける。複写機300にリーダー・ライタ303を設け、プラテンにセットされた文書のRFIDと、複写機300の前にいるユーザのRFIDとを読み取る。ユーザのRFIDから読み取った当該ユーザのアクセス権が、プラテン上の文書のRFIDから読み取った当該文書の機密レベルより高い場合にのみ、複写機300がその文書の複写を行えるように制御する。



## 【特許請求の範囲】

【請求項 1】 対象装置の要セキュリティ動作を管理するシステムであって、  
前記対象装置の近傍に設けられ、RFIDと通信を行ってそのRFIDが保持しているセキュリティ情報を取得するRFID通信手段と、  
前記RFID通信手段で2以上のRFIDから実質的に同時に取得したセキュリティ情報が、前記対象装置の前記要セキュリティ動作についての予め登録された許可条件を満足するか否かを判定する判定手段と、  
前記判定手段で前記許可条件が満足されたと判断した場合にのみ、前記対象装置に対して前記要セキュリティ動作の実行を許可する動作制御手段と、  
を備える装置セキュリティ管理システム。

【請求項 2】 前記許可条件は、前記要セキュリティ動作の対象物のセキュリティレベルとその動作を指示するユーザのセキュリティレベルとの関係が如何なる場合に前記要セキュリティ動作の実行を許可するかを示す条件であり、  
前記判定手段は、前記対象装置にセットされた対象物に付加されたRFIDから取得したセキュリティ情報と、ユーザが携帯するRFIDから取得したセキュリティ情報とから、各々のセキュリティレベルを求め、それらセキュリティレベルの関係が前記許可条件を満足するか否かを判定することを特徴とする請求項 1 記載の装置セキュリティ管理システム。

【請求項 3】 前記許可条件は、前記要セキュリティ動作の各対象物ごとに、その対象物の識別情報とその対象物に対する前記動作を許可するユーザの識別情報との対応を示した情報であり、  
前記判定手段は、前記対象装置にセットされた対象物に付加されたRFIDから取得したセキュリティ情報と、ユーザが携帯するRFIDから取得したセキュリティ情報とからそれぞれ識別情報を求め、それら識別情報が前記許可条件を満足するか否かを判定することを特徴とする請求項 1 記載の装置セキュリティ管理システム。

【請求項 4】 前記対象装置は複写機であり、  
前記判定手段は、前記複写機にセットされた原稿に付加されているRFIDから取得したセキュリティ情報と、ユーザのRFIDから取得したセキュリティ情報との組合せが、前記許可条件を満足するか否かを判定することを特徴とする請求項 1 記載の装置セキュリティ管理システム。

【請求項 5】 前記RFID通信手段のアンテナが、前記複写機の原稿フィードの原稿受け皿に取り付けられるとともに、この受け皿にユーザのRFIDをセットするためのくぼみを設け、前記アンテナにより前記受け皿上の原稿に付加されたRFIDと、前記くぼみにセットされたユーザのRFIDとに通信を行うことを特徴とする請求項 4 記載の装置セキュリティ管理システム。

【請求項 6】 前記RFID通信手段は、原稿が複写機にセットされた時に、その原稿に付加されたRFIDとユーザが携帯した当該ユーザのRFIDとを同時に読み取ることのできるように、前記原稿のRFIDを含む平面と前記ユーザのRFIDを含む平面から構成される角度の間になるよう設置された通信用のアンテナを有することを特徴とする請求項 4 記載の装置セキュリティ管理システム。

【請求項 7】 前記RFID通信手段は、複写機にセットされた原稿に付加されたRFIDを読み取るための第一のリーダ手段と、  
ユーザのRFIDを読み取ることのできる位置に設置された第二のリーダ手段と、  
を有することを特徴とする請求項 4 記載の装置セキュリティ管理システム。

【請求項 8】 前記許可条件は、前記RFID通信手段で同時に通信したRFIDの数と、それら各々のRFIDのセキュリティレベルとの関係から、前記要セキュリティ動作を許可する場合を規定した条件であり、  
前記判定手段は、前記RFID通信手段で同時に取得した1以上のRFIDの情報が、前記許可条件を満足するか否かを判定することを特徴とする請求項 1 記載の装置セキュリティ管理システム。

【請求項 9】 前記RFID通信手段は、セキュリティレベルがコピー可能なことを示すプロパティ情報を含んだ特定RFIDを、セキュリティレベルの情報を含んだ所定数の通常のRFIDと同時に読み取った場合、前記特定RFIDに対して前記通常のRFIDのセキュリティレベルを付与することを特徴とする請求項 1 記載の装置セキュリティ管理システム。

【請求項 10】 前記判定手段の判定で前記許可条件が満足されなかった場合に、その旨をユーザに通知する通知手段を有することを特徴とする請求項 1 記載の装置セキュリティ管理システム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 機密文書の複写など、セキュリティを要する装置の動作を制御するためのシステムに関する。

## 【0002】

【従来の技術】 機密文書は通常、文書上に「機密」または「複写厳禁」などのスタンプを押すなどすることでそれが明示されており、ユーザはその表示を見てその文書の複写などについて相応の注意を払っている。

【0003】 また、各ユーザに課金のために複写枚数を数えるカウンタを持たせ、そのカウンタを複写機にセットしないと複写機が作動しないシステムがある。このシステムは、カウンタを持っている部内者しか複写ができないという意味ではセキュリティの効果をもたらしている。

【0004】また、人的資源に頼った方式として、機密文書の保管してある部屋をガードマンやそれに類する人によって管理することがよく行われている。また、複写担当者を介してしか文書複写をできないような運用を行っている場合もある。

【0005】また近年では、機密文書を、紫外線や赤外線などの非可視光の下でしか読めないような特殊なインクを使って印刷することも行われている。この場合、専用光源のある閲覧室では機密文書を読むことができるが、その機密文書を一般の複写機で複写しようと思っ

ても、一般の複写機は可視光線の反射波を利用するので、可視光線を反射しにくいインクを使った機密文書は複写できない。

【0006】しかしながら、全く何もできなることによる不便さや、その特殊な文書を作る煩わしさが汎用の妨げとなっている。

【0007】  
【発明が解決しようとする課題】「機密」等の表示を行う方式は、ユーザのモラルに頼った方式であり、セキュリティ面から見て十分とは言えない場合が多い。

【0008】各ユーザに複写カウンタを持たせる方式は、カウンタさえ持っていればどのような文書でも複写できるので、機密文書の複写管理という観点からは十分なセキュリティが確保できているとは言いがたい。

【0009】ガードマン等により管理を行う方式は、コスト面で問題が多く、また結局は人間のモラルに頼っているといえる。

【0010】また、機密文書に特殊インクを用いる方式は、不正複写防止という観点から見れば高いセキュリティが得られるが、正当なユーザが不便を強いられるという問題がある。すなわち、特殊インクを使った場合、機密文書を読むのにも特殊な光源を要し、また機密文書を印刷するのにも特殊な複写機を要する。

【0011】このように従来の機密文書の複写の管理方式は、いずれも問題があった。以上、機密文書の複写の場合を例にとったが、ユーザに対して提供するサービスにセキュリティの管理を要する状況は多々あり、そのようなセキュリティ管理を自動化した例も、例えば機密区画の入退室管理装置などのように多い。このようなセキュリティに係る装置の動作管理は、例えばユーザにICカードを持たせ、このカードを装置に挿入するなどの方式で行われているが、それだけでは不十分な場合や、不便な場合もある。例えば複写の場合で言えば、文書の機密の程度によってどのレベルのユーザまで複写を許すかなどの、きめ細かい管理を行うには、ICカード等でユーザ確認を行うだけでは不十分である。また、例えば、入退室管理装置では、ビジター（一時的な訪問者）の出入りのために有効なカードを持つホスト側の人間が付き添っていないとできないなどの不便がある。

【0012】本発明はこのような問題に鑑みなされたも

のであり、セキュリティを要する装置の動作をきめ細かく制御するための仕組みを提供することを目的とする。

【0013】

【課題を解決するための手段】上記目的を達成するため、本発明に係る装置セキュリティ管理システムは、対象装置の要セキュリティ動作を管理するシステムであって、前記対象装置の近傍に設けられ、RFIDと通信を行ってそのRFIDが保持しているセキュリティ情報を取得するRFID通信手段と、前記RFID通信手段で2以上のRFIDから実質的に同時に取得したセキュリティ情報が、前記対象装置の前記要セキュリティ動作についての予め登録された許可条件を満足するか否かを判定する判定手段と、前記判定手段で前記許可条件が満足されたと判断した場合にのみ、前記対象装置に対して前記要セキュリティ動作の実行を許可する。

【0014】このシステムによれば、対象装置に関わる複数のRFIDの情報に基づきその装置の動作が制御できるので、きめ細かなセキュリティ管理が可能になる。

【0015】本発明の好適な態様では、前記許可条件は、前記要セキュリティ動作の対象物のセキュリティレベルとその動作を指示するユーザのセキュリティレベルとの関係が如何なる場合に前記要セキュリティ動作の実行を許可するかを示す条件であり、前記判定手段は、前記対象装置にセットされた対象物に付加されたRFIDから取得したセキュリティ情報と、ユーザが携帯するRFIDから取得したセキュリティ情報とから、各々のセキュリティレベルを求め、それらセキュリティレベルの関係が前記許可条件を満足するか否かを判定する。

【0016】この態様では、要セキュリティ動作の対象物のRFIDと、ユーザのRFIDから各々のセキュリティレベルを取得し、それら両者の関係に基づきその動作の実行が許可できるかを判定する。例えば複写機を例にとった場合、複写機が対象装置に対応し、機密文書の複写動作が要セキュリティ動作に、機密文書がその対象物に、それぞれ対応する。この態様によれば、対象物とユーザの関係に基づき、要セキュリティ動作の実行を詳細に管理できる。

【0017】別の好適な態様では、前記許可条件は、前記RFID通信手段で同時に通信したRFIDの数と、それら各々のRFIDのセキュリティレベルとの関係から、前記要セキュリティ動作を許可する場合を規定した条件であり、前記判定手段は、前記RFID通信手段で同時に取得した1以上のRFIDの情報が、前記許可条件を満足するか否かを判定する。

【0018】この態様では、例えば複数人で相互の信用保証が期待される場合などにも一定の要セキュリティ動作の実行が可能になり、一人の認証情報に基づき要セキュリティ動作を行っていた従来の管理方式に比べて、現場のニーズに合わせたきめ細かな動作許可の条件設定が可能になる。

【0019】また別の好適な態様では、前記RFID通信手段は、セキュリティレベルがコピー可能なことを示すプロパティ情報を含んだ特定RFIDを、セキュリティレベルの情報を含んだ所定数の通常のRFIDと同時に読み取った場合、前記特定RFIDに対して前記通常のRFIDのセキュリティレベルを付与する。

【0020】この態様では、特定RFIDと所定数の通常のRFIDとをほぼ同時にRFID通信手段の通信範囲内に入れるだけで、通常のRFIDのセキュリティ情報をその特定RFIDにコピーできるので、入退室管理システムなどにおいて、訪問者やIDカードを忘れた者等に対して発行する仮カードに対してその者が必要とするセキュリティ許可内容を書き込むのが容易になる。

【0021】

【発明の実施の形態】〔実施形態1〕本実施形態では、複写機による機密文書の複写管理を例にとる。したがってこの実施形態では、複写機が特許請求の範囲の「対象装置」に該当する。ここでは説明を簡単にするため、セキュリティ管理のための情報処理装置および記憶装置は、複写機とは別体のパーソナルコンピュータをベースに構築されているとする。ただし、最近の複写機は、内部に高性能のMPUや大容量の記憶装置を有している場合が多く、以下に説明するセキュリティ管理の情報処理機能を複写機に組み込むことは容易である。

【0022】本実施形態では、セキュリティ管理のためにRFID(Radio Frequency Identification)を用いる。RFIDは、非接触読取型のデータキャリアであり、記憶用のICチップと通信用のアンテナとを内蔵する。RFIDは、プラスチックカード形式のものが一般的であるが、可換性をもつ薄いタグの形のものも開発されている。記憶容量の小さいRFIDはトランスポンダーと呼ばれることもある。RFIDはその通信方式(利用する通信周波数等)によって、主に4種類のものに分類される。この分類は、RFIDとそれに読み書きを行うリーダ・ライタとの通信距離に応じて名付けられており、通信距離が短い順に、密着型、近接型、近傍型、マイクロ波型と呼ばれている。密着型は短波の静電誘導を利用したもので、その通信距離は数ミリである。近接型は短波の電磁誘導を利用したもので、その通信距離は1cmから30cmくらいである。近傍型は長波の電磁誘導を利用したもので、その通信距離は30cmから70cmくらいである。マイクロ波型は文字どおりマイクロ波の電磁誘導を利用したもので、通信距離は3mから10mくらいである。マイクロ波型のICカードは電源として電池を利用する人が多いが、他の3つの型のカードはリーダ・ライタからの電磁誘導等により電源を得る無電池のものが普通である。本実施形態では、近傍型乃至マイクロ波型の使用を想定する。

【0023】図1に示すように、本実施形態のシステムは、一つの機密室100内に構築される。複写管理の対

象となる機密文書は書棚108に保管されている。図2に示すように、機密文書200には、RFID201が貼付されている。書棚108と複写機106は同じ機密室100内にあり、その入り口はリーダ・ライタ103のついたドア107で守られている。

【0024】リーダ・ライタは、ドア107の部分だけでなく、複写機106と書棚108にも設けられている(リーダ・ライタ102及びリーダ・ライタ109)。各リーダ・ライタ102、103、109は、セキュリティ管理装置104に接続されている。セキュリティ管理装置104には、各ユーザや各文書のID番号や後述する機密文書の複写許可の条件などを記憶した記憶装置105が接続されている。各リーダ・ライタは、例えば一定間隔(例えば数十ミリ秒から数秒程度)ごとに、あるいは特定のイベントが発生したときに、質問波を発する。リーダ・ライタの通信可能な範囲内にRFIDがあれば、そのRFIDは自己の保持するデータで変調した応答波を返信する。各リーダ・ライタは、この応答波を受信すると、その応答波に含まれるデータを抽出し、セキュリティ管理装置104に送信する。

【0025】図2に示すように、各ユーザ202は、RFID203を携帯するものとする。もし、RFID203を携帯しないユーザが機密文書を持ち出そうと思っても、リーダ・ライタ103で有効なRFID203を検知しない限りセキュリティ管理装置104はドア107の開動作を許可しないので、そのユーザは機密室100内に入れない。また有効なRFIDを携帯するユーザでも、機密文書のセキュリティレベルを満足しない者が機密文書を機密室100から持ち出そうとすると、セキュリティ管理装置104はドア107を開かないようにする。もちろん、入室する場合にも携帯するRFIDのセキュリティレベルをチェックしてドアの開閉を行うようにする。

【0026】なお、リーダ・ライタは通常、RFIDと電波で通信するアンテナと、このアンテナで送信する質問波や受信する応答波を処理したり、セキュリティ管理装置104とデータのやり取りを行う制御部から成り立っている。以下では、詳細が必要でない場合は、リーダ・ライタのアンテナ、制御部などと区別して書くことはせず、単にリーダ・ライタと書くことにする。

【0027】複写機106に取り付けられたリーダ・ライタ102は、複写のためにセットされた機密文書のRFID201とユーザのRFID203を実質的に同時に読み込めるように配設されている。

【0028】リーダ・ライタ102のアンテナは、図3(a)に示すように、複写機300において、複写される原稿を押さえるカバー302に埋め込まれている。図3(b)は、複写機300のカバー304の押さえ側の面にリーダ・ライタの別の形(矩形)のアンテナ305を設けた例を示す。ユーザは、原稿を複写面301上に

置いてこのカバー302を閉めたのち、そのカバー302上に、自分のRFID203を置く。すると、リーダー・ライタ102は、複写面上の原稿に取り付けられたRFIDと、カバー302上のユーザRFIDと通信（質問波と応答波のやり取り）を行い、各々の保持するセキュリティ情報を取得し、管理装置104に送る。なお、セキュリティ管理装置104は、ユーザのRFIDが検知されない（すなわちユーザRFIDのセキュリティ情報がリーダー・ライタ102に届かない）時には、複写機106に対して複写を許可しない。すなわち、機密室100内の複写機106は、基本的にセキュリティ管理装置104から動作許可を受けない限り、複写動作を実行できないように構成されている。

【0029】機密文書のRFIDとユーザのRFIDが保持するセキュリティ情報のデータ構造は、例えば図4に示すようなものである。すなわちセキュリティ情報は、RFIDの固有のID番号401とセキュリティレベル402から成り立っている。ID番号401が、そのRFIDが貼付された文書、あるいはそのRFIDを携帯するユーザの識別情報となる。セキュリティ情報は、これ以外にも各種のデータを含みうるが、本実施形態に関わるのはこの2つのデータなので、ここではそれらを挙げるにとどめる。

【0030】セキュリティレベル402は、文書の場合は例えばその文書の機密の度合いを表す正の整数であり、例えばその数値が大きいほど機密度が高い。一方、ユーザのRFIDのセキュリティレベル402は、ユーザが取扱を許されている最高の機密度を表す数値である。したがって、ユーザのRFIDのセキュリティレベルが、文書のRFIDのセキュリティレベル以上でない場合、ユーザはその文書を持ち出したり、複写したりできないように管理される。すなわち、機密文書のセキュリティレベルがKで、ユーザのセキュリティレベルがMの場合、 $M \geq K$ の時に限って複写機が動作するようにする。

【0031】RFIDを用いた複写管理のプロセスを図5に示す。図5のフローチャートは、管理装置104の処理動作を示している。ユーザが、複写機106のスタートのボタンを押すと、このイベントが複写機106のコントローラから管理装置104にその旨が伝わる。これを受けた管理装置104は、複写機106のリーダー・ライタ102に対して、質問波発射の命令を送る（ステップ1001）。この命令を受けたリーダー・ライタ102はアンテナから質問波を送り、これに対する複写面301に置かれた機密文書のRFIDとカバー302の上に置かれたユーザのRFIDからの応答波を受け取る

（ステップ1002）。応答波が無ければ（すなわちリーダー・ライタ102から、RFIDのセキュリティ情報が伝送されてこなければ）、ステップ1002の判定結果が否定（N）となり、この場合管理装置104はなに

もせずに処理を終了する。従ってこの場合複写機106には複写動作の許可が与えられないので、複写機106は複写は行わず、待機状態となる。応答波があれば、管理装置104は、その応答波のセキュリティ情報から文書及びユーザのセキュリティレベルをそれぞれ求め、両者を比較する（ステップ1003）。もしユーザのセキュリティレベルが文書のセキュリティレベル未満であれば、ステップ1003の判定結果が否定（N）となる。この場合は、管理装置104は何も行わずに処理を終了する。すなわちこの場合、管理装置104から複写機106に複写動作許可の信号が送られないので、複写機106は複写動作禁止のまま待機する。ステップ1003の判定で、ユーザのセキュリティレベルが文書のセキュリティレベル以上であれば、ステップ1004に移り、管理装置104は複写機106に対して複写動作許可命令を送る。これにより、複写機106は複写動作が可能な状態となり、複写面301上の文書の複写を行う。複写が終われば、管理装置104は、再び、複写機106からスタートボタン押下イベントを報せる通知を待つ状態となる。

【0032】以上のような処理により、機密文書の機密度と、ユーザに与えられた機密アクセス権との両方を考慮した、きめ細かい複写管理を行うことができる。

【0033】また、本実施形態のシステムでは、以上のようなセキュリティレベルを利用した複写管理の他に、文書毎に特定のユーザに限って複写を許すような管理も可能である。この場合、管理装置104に、許可条件を表す図6に示すようなテーブルを設ける。図6には3種類のテーブルの例を示している。テーブル（a）では、各機密文書ごとに、そのIDと、その機密文書の取扱（複写や持出）を許可するユーザのIDとが登録されている。このテーブルを用いて管理を行う場合、管理装置104は、複写機106のリーダー・ライタ102から送られてきた文書及びユーザのRFIDのセキュリティ情報から、文書及びユーザのID番号をそれぞれ抽出し、このテーブルを参照してそのユーザがその文書の複写を許可されているかどうかを判定する。したがって、この方式の場合は、RFIDにはID番号の情報のみが含まれていればよく、セキュリティレベルの情報は必要ない（図4の例と比較）。

【0034】図6の（b）のテーブルは、文書のセキュリティレベルごとに、そのレベルの文書に対する取扱を許すユーザのIDが登録されている。この場合、管理装置104は、リーダー・ライタ102から受け取った文書のセキュリティレベルの情報とユーザのID番号の情報から、このテーブルを参照してそのユーザがその文書の複写を許可されているかどうかを判定する。

【0035】図6の（c）のテーブルは、各文書ごとに、そのIDと、その文書に対する取扱を許すユーザのセキュリティレベルの条件が登録されている。この場

合、管理装置104は、リーダー・ライタ102から受け取った文書のID番号とユーザのセキュリティレベルから、そのユーザがそのテーブルに示されている条件を満足しているかどうかを判定する。

【0036】管理装置104は、このようなテーブルに基づく判定の結果、複写の許可条件を満足していれば、複写動作許可信号を複写機106のコントローラに送る。そうでなければ、管理装置104は何もせず、その結果複写機106は動かないままとなる。

【0037】一つの方式としては、複写が一回行われる度に、複写機106のコントローラは、デフォルトの複写動作不可状態とする。そして、ユーザが複写スタートのボタンを押す度に、文書に付加されたRFIDとユーザのRFIDとが読み直されるようにする。なお、これはあくまで一例である。

【0038】なお、機密文書を保管する書棚108に扉とリーダー・ライタ109を設け、セキュリティ管理装置104でその扉の開閉等を制御することで、より高度の機密を保てる。すなわち、リーダー・ライタ109で書棚108の近傍に来たユーザのRFIDのID番号を識別するようにし、ID番号が検知できなかった場合には扉が開かないようにするなどである。この方式では、書棚108を開けたユーザのIDを管理装置104で記録することもできる。また更には、書棚108からユーザが取り出そうとした文書のRFIDをリーダー・ライタ109で読み取り、複写管理の場合と同様、その文書とそれを取り出そうとしたユーザのセキュリティレベルを検査し、そのユーザがアクセスを許可されていない文書であることが判明した場合には、管理装置104からしかるべき管理者に警報を発するなどの処置がとれる。

【0039】このように、本実施形態では、機密文書の複写に関して、ユーザ及び文書の両面からきめ細かい機密管理を行うことができ、機密事項の不要な漏洩を防ぐことができる。

【0040】【実施形態2】この実施形態は、複写管理におけるユーザRFIDの取扱に関するものであり、請求項5に関わる。

【0041】本実施形態では、図7に示すように、複写機500（上部構造のみ図示）のリーダー・ライタのアンテナ502を、原稿フィード501の原稿受け皿に装着する。この構成において、リーダー・ライタのアンテナ502は、フィード下部の原稿スキャン位置の部分のカバーするように取り付けられる。ユーザのRFIDは、フィード501の受け皿に設けられた窪み503に置いてもらう。この上に複写したい文書を置いてもらえば、複写動作に支障を来さず、ユーザと文書のRFIDの両方を読み取ることができる。この場合、一枚でも読み込み不可の原稿が生じると複写が出来なくなる。一枚一枚調べて複写可能か調べるには次のようにする。

【0042】すなわち、別のアンテナ配置として、受け

皿上の原稿が複写面（プラテン）まで搬送される際に回転して通るフィード501のコーナー部504をカバーする位置にアンテナを設けることも好適である。この場合ユーザのRFIDは、フィード501のコーナー部分504の上に置いてもらうようにすればよい。この場合も、複写時の原稿搬送を妨害することなく、原稿及びユーザのRFIDの読み取りを行うことができる。

【0043】本実施形態のセキュリティ管理処理は、基本的に実施形態1と同様である。ただし、原稿を自動送りする原稿フィード501を用いるので、セキュリティ管理装置104はこの点の配慮した制御を行う。

【0044】すなわち、複写機の制御状態は複写が一枚行われるごとに複写禁止状態にリセットする。そして、文書をフィードして読み取る際に、その文書のRFIDを読み取ってそのセキュリティレベルを確認する。ここで、セキュリティレベルのチェックで、そのユーザがその文書を複写できないと判定された場合、例えば、その文書を複写することなく排紙し、次の文書をフィードするようにすることが好適である。この場合、書類の読み取りを中断することなく、複写可能なものだけ複写出来る。

【0045】この処理の手順は、図5に示した実施形態1の処理手順アルゴリズムにおいて、ステップ1001の前に『文書を一枚複写面にフィードするという命令を複写機のコントローラに送る』というステップを加え、終了の処理の代わりにループを作り、上記のフィード処理の前にアルゴリズムのコントロールが戻るようにすれば実現できる。原稿をフィードしても何も送られなくなった時点で、アルゴリズムを終了させればよい。

【0046】この実施形態によれば、複数の文書を、機密管理しつつ、連続的に複写することができる。

【0047】【実施形態3】この実施形態は、複写機のリーダー・ライタのアンテナ構成の別の形態に関するものであり、請求項6と7に関する。

【0048】実施形態1及び2では、ユーザは携帯するRFIDを複写機の上に置かねばならなかった。この例ではユーザがRFIDを携帯したまま複写が可能のようにアンテナを配置する。

【0049】第一の方式は、文書を読むリーダー・ライタの他に、ユーザ用の第二のリーダー・ライタを、例えば複写機の手前側に取り付けるといったものである。文書用のリーダー・ライタとユーザ用のリーダー・ライタは、通信領域が異なるので同時に電波を送り、読み取りが開始できる。ユーザ用のリーダー・ライタのアンテナは、図3で言えば、複写機の上面と前面の交わる角の部分304に設ける。このアンテナとしては、複写機の前に立ったユーザのRFIDの位置（例えばユーザの胸から腰の辺り）をカバーする程度の通信距離のものを選べばよい。

【0050】第二の方式では、ループアンテナを複写機の前面に付ける。ループアンテナは通常その前と後ろに



同じ形で通信領域ができるので、一方は複写機上の文書のRFIDを読むことができ、もう一方の通信領域で、腰につけたユーザのRFIDを読むことが出来る。なお、複写機は金属でできており、この通信領域は金属によって影響を受けるので通信電力やアンテナの形状や設置場所に充分注意を要する。また、複写に用いるトナーは帯電しているので、トナーが付けられるローラーの部分に電波が行かないように工夫する必要がある。例えば、アンテナの複写機内部側の一部を金属などで遮蔽すればよい。

【0051】第三の方式は、ループアンテナの一つの通信領域で2つのRFIDを読みとるというものである（上記第二の方式では、ループアンテナの両側にできる2つの通信領域で2つのRFIDを読み取った）。この方式では、アンテナの向きを充分に考慮する必要がある。ここで、アンテナの「向き」とはアンテナのデバイスから通信距離が最大になる方向のことを言う。アンテナがループ状の場合、アンテナの向きはループを含む平面に対し垂直の方向になる。もし、アンテナの向きがユーザの携帯するRFID（のアンテナ）に平行であれば、ユーザのRFIDの小アンテナにアンテナからくる磁束が通りにくくなり、ユーザのRFIDが読み取りにくくなる（一般に複写面上の文書は水平であり、ユーザが携帯するRFIDは垂直（首から下げるなど）である）。またアンテナの向きを、複写面に平行にすると、文書のRFIDに対してアンテナの向きが平行になり、今度は同様に文書のRFIDが読みにくくなる。従って、アンテナをユーザのRFIDの向きと複写面の向き（これらは互いに直角）の両方に平行にならないように設置すれば、上記のような問題は解消される。例えば、複写面によって規定される水平面と、複写機前面に立ったユーザに向かい合う垂直面と、のそれぞれから45度の角度になるようにアンテナの向きを設定すれば、ユーザ、文書双方のRFIDが読めることになる。図示すれば、図8に示すように、リーダー・ライタのアンテナは、RFID1101が取り付けられた文書1105がセットされる複写機1100の複写面によって規定される水平面と、その前（操作パネル側）に立ったユーザ1104（RFID1102）に対向する垂直面との間の90度の角度の範囲1103のなかで、できるだけ45度に近い向きに配設すればよい。

【0052】この実施形態によれば、一つのリーダー・ライタで、ユーザがRFIDを複写機上に置くなどの煩雑な動作をすることなく、ユーザのRFIDと文書のRFIDと同時に読むことができ、複写機の機密動作制御ができる。

【0053】〔実施形態4〕この実施形態は請求項8に関する。

【0054】通常、入退出管理システムでは、一人のユーザがRFIDを内蔵するカードを入り口ドア付近に設

置されたリーダー・ライタにかざすことで、ドアの開動作を要求する。このとき、リーダー・ライタはRFIDのセキュリティ情報を読み取り、その情報をセキュリティ管理装置（例えば図1の装置104）に送る。管理装置は、そのセキュリティ情報の中のID番号が、その部屋の中へのアクセスが認められた正当なIDであるかどうかを、所定の管理データ・ベースを参照して判定し、正当なIDであれば、ドアを開け、そうでなければドアを開けない。

10 【0055】この方式は、非常に厳格な管理方式であり、場合によっては厳格すぎて不便になることもある。例えば、たまたまカードを忘れた場合、機密室100に入ることが出来ず、必要な作業ができなくなることも考えられる。このような場合、仮のIDカードを発行してそのユーザにもってもらいなどの対処を行うことが多いが、1つの建物内に機密レベルの異なる複数の部屋がある場合も多く、そのような場合仮のIDカードでは、当人の本当のIDカードと同様のセキュリティクリアランスが得られない場合があつて不便になることがある。

20 【0056】また、入退室管理装置では、一般に、一人が有効なカードを持っていれば、それに同行した人はカードを持たなくても、カードが持っている人がドアを開けることによって同行者の入室が可能である。ただし、この場合も、有効なカードを持った特定の人（ガードマンなど）が居ないと、その人が来るまで大変な時間を待たされるということがあり、不便である。

【0057】さて、機密度の高い部屋は、一般に利用する人が限られている。したがって、利用者が2人またはそれ以上いる場合、特別の管理者が居なくても、互いが信用保証をすることができる。すなわち、機密度の高い部屋の利用者は互いを知っていることが多く、お互いの信用を保証できる場合が多い。したがって、複数人の利用者の信用度によって入室を可能にすることにより、セキュリティを保証しながら利便性を達成することになる。本実施形態では、この考え方に従って、セキュリティと利便性のある程度まで両立した入退室管理を行う。

30 【0058】なお、このように、2人以上いればセキュリティの保証がなされてある物事がなされる例はいくつもある。例えば、銀行の旧来方式の貸し金庫なども、本人の鍵と銀行側の鍵があつて初めて、該金庫を開けることができ、これは複数人による信用保証の一種と考えられる。

40 【0059】また、危険物あるいは劇薬などの管理室に入るのに、その部屋は特定の人しか利用しないのに、いちいちガードマンに許可をもとめ、ドアを開けるなどの処置がなされる場合がある。これも利用者が数人が居ることで、互いの信用保証を獲得するようにすれば、入室が可能となり利便性が増すとともに、場合によってはガードマンを廃止して人権費を減らすこともできる。病院などでは、癌患者や難病者の苦痛を押さえるためにモル

ヒネを利用することがある。このモルヒネは麻薬とも見られているので院長しかモルヒネを保管している金庫が開けられないことが多い。しかし、夜中や院長が居ない場合に突然モルヒネが必要となる場合がある。例えば、医師二人がいれば、または医師一人と看護婦2人がいれば、金庫を開けても良いなどのルールを決め、そのルールに従って管理が行えれば、緊急の際の利便性が向上するのは言うまでもない。

【0060】また、上記実施形態1, 2, 3では、一方のRFIDは書類に付加されたものであるが、もう一方はユーザの携帯するRFIDであり、両者がセキュリティレベルが満足されたときのみ複写機を動かすことができた。両者のRFIDはそれを保持するもの(属性)が違いますが、セキュリティのコントロールの面やコントローラの制御のアルゴリズムにおいては、実施形態1, 2, 3も複数のRFIDのセキュリティ情報の関係に基づき、管理対象の装置の動作を管理するシステムの一つと捉えることができる。

【0061】ユーザに付与されるセキュリティレベル(機密アクセス権)にはいくつかの段階がある。どのようなセキュリティレベルの人がどれだけ集まれば信用保証がなされ(入室や金庫扉のオープン、その他の処理が認められ)るかのルールを定めておき、リーダー・ライターで同時に読みとった各人のRFIDのセキュリティレベルがそのルールを満足するかをセキュリティ管理装置104で判定して入室等の処理を管理すれば、きめ細かなセキュリティ管理が可能である。

【0062】ルールとしては、例えば単純な例としては、一番高いセキュリティレベルでは一人で入室(または処理)が可能になり、二番目のレベルではK(>1)人以上いれば入室が可能になり、それ以下のレベルでは入室が不可であるというようなルールが考えられる。以上は非常に単純な例であったが、医師1人と看護婦2人以上が同時にいれば金庫を開けるのを許す、という場合なども、セキュリティレベルを用いてルール化できることは明らかであろう。本実施形態では、このような複数人のセキュリティレベルの組合せに基づいて、ドア開閉などの所定の処理動作を制御する機構を提供する。

【0063】本実施形態の処理手順は、図9～図11のフローチャートに示される。以下では、入室管理における入り口ドアの開閉装置の制御を例にとって説明するが、同様のセキュリティ管理が複写機その他セキュリティ管理を要する装置の動作制御に応用可能なことは以下の説明から容易に理解されるであろう。

【0064】以下、本実施例のアルゴリズムを図9～図11のフローチャートに基いて説明する。ここでは入室管理を例にとるので、システム構成としては図1を参照されたい。

【0065】図9に示すように、入り口のリーダー・ライター103は一定間隔で質問波を繰り返し送信し、RFI

Dからの応答波を確認している(ステップ601)。応答波が無ければステップ601の判定が否定(N)となり、ループが繰り返される。

【0066】応答波があった場合、セキュリティ管理装置104は、確認できたRFIDが1つだけか否かの判定をステップ602にて行い、RFIDが一個しか確認できない場合は、ステップ603に移行し、2個以上確認できる場合には、ステップ604に移行する。ステップ603の手続きの詳細は図10のフローチャートで記述され、ステップ604の手続きの詳細は図11のフローチャートで示される。

【0067】図10を参照してステップ603の詳細な手順を説明する。この手順は、リーダー・ライターがRFIDを一つしか確認しなかった場合である。この場合、セキュリティ管理装置104は、ステップ701で、確認したRFIDのセキュリティレベルが、入り口ドアの開動作の許可を受けられるレベルかどうかを判断される。

【0068】もし、許可を受けられるレベルであれば、制御の対象の装置(ここではドアの開閉装置)のコントローラに動作許可の命令を送る(ステップ702)。そうでなければ、対象装置に動作許可を送らず、警告処理等のエラー処理を行う(ステップ703)。ステップ703の場合、対象装置であるドア開閉装置は動作許可を得ていないので、ドアを開かない。ステップ702又は703が終わると、ステップ601に戻る。

【0069】図11を参照して、ステップ604の詳細な手続きを説明する。この手順は、RFIDが複数枚確認出来る場合の処理である。この場合、管理装置104は、ステップ801で、同時に確認できた複数のRFIDのセキュリティレベルが、予め管理装置104に登録されている対象装置(ドア開閉装置)の動作許可条件を満たしているかどうかを判定する。図11の例では、前に例示した単純なルール(あるレベルの人がK人以上居ればよい、というルール)の場合を示している。この場合、ステップ801にて、所定のセキュリティレベル以上のRFIDがK枚以上あるかを判断する。もしそうであれば(ステップ801の結果がY)、対象装置であるドア開閉装置のコントローラに動作許可の命令を送る(ステップ802)。

これにより、入り口のドアが開かれ、人々が室内に入れるようになる。ステップ801の判定結果が否定(N)の場合、警告処理等のエラー処理を行う(ステップ803)。この場合、ドア開閉装置は動作許可を得ていないので、ドアは開かない。ステップ802又は803が終わると、ステップ601に戻る。

【0070】以上は単純な例で説明したが、ステップ801の動作許可の判定のためのルールには、様々なバリエーションが考えられる。例えば、「レベル3～5の人が1人以上かつレベル1～2の人が2人以上いれば、許可する」など、各セキュリティレベルごとに必要とする人数を定めるルールも考えられる。また、セキュリティ

レベルの値をポイントと考え、同時に読み取ったRFIDのセキュリティレベルの総和が、所定のしきい値以上となったら許可する、等のルールも考えられる。

【0071】このように、本実施形態によれば、複数人のセキュリティレベルの関係から対象装置（例えばドア開閉装置）の動作を制御できるので、1人の人間のセキュリティ情報のみに基づいてセキュリティ管理を行っていた従来システムに比べ、より柔軟なシステムが構築できる。

【0072】〔実施形態5〕この実施形態は請求項9に 10 関わる。

【0073】入退室管理において、ビジター（訪問者）は、一般の場合、有効なIDカード（RFID）を持った関係者が同行することで入室を可能にすることが多い。関係者であっても、RFIDのカードを忘れた場合は、ガードマンに入れて貰ったり、守衛所で名前を登録してドアの開閉不可能なバッジ等が支給されたりする。いずれにせよ、ドアのところで誰かに開けて貰わなければならない。特に関係者本人がIDカードを忘れた場合、不便であり、生産性が下がる。

【0074】そこで、本実施形態では、ビジターやRFIDカードを忘れた関係者に対し、仮のRFIDを発行し、その仮カードに対して、他の関係者からの認証により、セキュリティレベルを自動付与する機構を提供する。すなわち、本実施形態では、他の関係者が所定人数以上認めれば、ビジター等に対してそれら関係者と同等のセキュリティレベルを自動付与する。他の関係者たちの認証は、ビジターがそれら関係者たちと同行してリーダー・ライタの通信範囲内を通過するときに、自動的に行われるようにする。すなわち、例えばオフィス等に入る 30 ために、入り口のリーダー・ライタの近傍に、仮のRFIDを持った人と、その人の認証に要する所定人数の関係者とが来れば、リーダー・ライタでそれを検知して、仮のRFIDにそれら関係者と同等のセキュリティレベルの情報をリーダー・ライタから書き込むようにする。

【0075】これは先に述べた実施形態4の場合と似ている。異なる点は他に所定人数居ればドアが開くのではなく、ドアを開けることのできる別のRFIDを作る

（より厳密にはRFIDにドアを開けることができるセキュリティレベルを付与する）という点である。

【0076】ただし、どんなカードでもそのセキュリティレベルがコピーできると、高いセキュリティレベルのカードをなんらかの方法で入手してそのレベルを自分のものにコピーできてしまう。このような不正使用を防止しようとするならば、例えば仮のRFIDカードに、仮のカードであることを示すセキュリティ上のプロパティ情報を持たせればよい。こうすることにより、セキュリティレベルのコピーは、限定された特殊な仮のカードだけにしかコピーできない。なお、仮のカード自体は、守衛所などで一定の手続を踏んで交付されるものなので、 50

かなりのレベルのセキュリティが確保されている。仮のカードの有効期限を例えば1日限りなどと限定しておけば、更にセキュリティが向上する。

【0077】本実施形態の処理は次のようになる。すなわち、セキュリティ管理装置104が、あるリーダー・ライタから、同時に読み取った複数のRFIDのセキュリティ情報を取得した場合、その中に仮のRFIDのセキュリティ情報が含まれているかどうかを判定する。仮のRFIDかどうかは、前述した仮カードを示すプロパティ情報が含まれているかどうかで判定してもよいし、仮RFIDに使うID番号を予め限定してそれを管理装置104に登録しておき、読み取ったRFID群の中にそれに該当するものがあるかどうかで判定してもよい。同時に読み取ったRFID群の中に、仮のRFIDがあれば、管理装置104は、同時に読み取った他のRFID群セキュリティレベルの値を、リーダー・ライタを介してその仮のRFIDに書き込む。

【0078】一般に、RFIDを忘れた者は、同部署の者に同行を求めれば、ほとんど自分自身のものと同等のセキュリティレベルを仮RFIDにコピーできるので、その日の業務の支障が大幅に減る。

【0079】本実施形態によれば、有効なRFIDを持つ者と同行するだけで、仮のRFIDにその者と同等のセキュリティレベルを自動書き込みできるので、仮カード発行場所ですべてのセキュリティ設定を手で行うなどの手間なしで、所望のセキュリティを実現できる仮のRFIDが得られる。

【0080】〔実施形態6〕この実施形態は請求項10に関する。実施形態1、2、3において、ユーザのセキュリティレベルが文書のセキュリティレベル未満の場合、複写がなされない。この場合、本実施形態では、セキュリティ管理装置104から複写機106に対して、複写許可条件が満たされないことを示すエラーコードを送る。このエラーコードを受け取った複写機106のコントローラは、それに基づいて、複写機に設けられる操作パネルの液晶表示装置などに、そのコードに対応した例えば図12に示すような複写不可のメッセージを表示する。可視的表示の代わりに、複写機106に音声発生装置を付け、音声でもってユーザに複写不可の旨を通知するようにしてもよい。

【0081】この実施形態によれば、ユーザは、どのような理由で複写機を使えないかを知ることができ、知らないがゆえに起こる時間の無駄が省ける。

【図面の簡単な説明】

【図1】 本発明に係る複写管理を適用した機密室の構成を示す図である。

【図2】 ユーザ及び機密文書とそのRFIDを示す図である。

【図3】 リーダー・ライタを装着した複写機の概略を示す図である。

【図4】 RFIDが持つセキュリティ情報のデータ構造の一例を示す図である。

【図5】 セキュリティ管理装置による複写機のセキュリティ制御の手順を示すフローチャートである。

【図6】 複写動作の許可条件のテーブルの例を示す図である。

【図7】 実施形態2のリーダー・ライタのアンテナ配置の一例を示す図である。

【図8】 実施形態3のリーダー・ライタのアンテナ配置の一例を示す図である。

【図9】 実施形態4のシステムの全体的な処理手順を示すフローチャートである。

【図10】 実施形態4のシステムで、RFIDが1つ

しか検出できなかった場合の処理を示すフローチャートである。

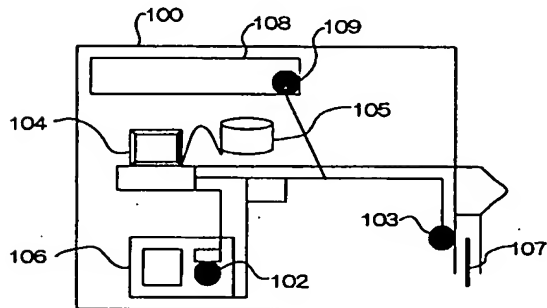
【図11】 実施形態4のシステムで、RFIDが2以上検出できた場合の処理を示すフローチャートである。

【図12】 実施形態6における複写不可の表示の例を示す図である。

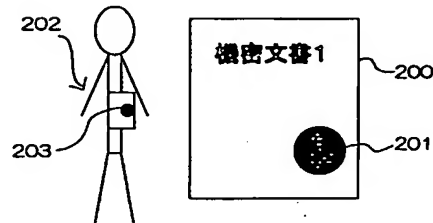
【符号の説明】

100 機密室、102, 103, 109 リーダ・ライタ、104 セキュリティ管理装置、105 記憶装置、106 複写機、107 ドア、108 書棚、201, 203 RFID、300 複写機、301 複写面、302カバー、303 リーダ・ライタ。

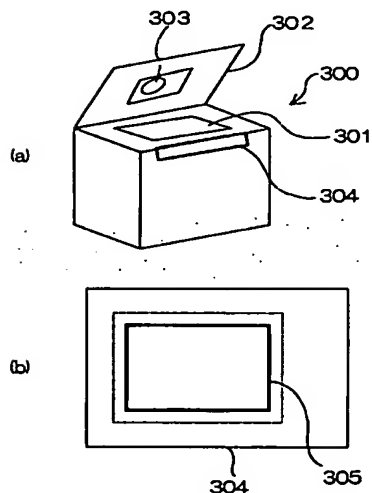
【図1】



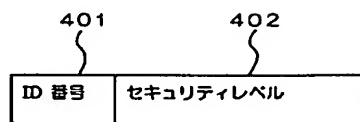
【図2】



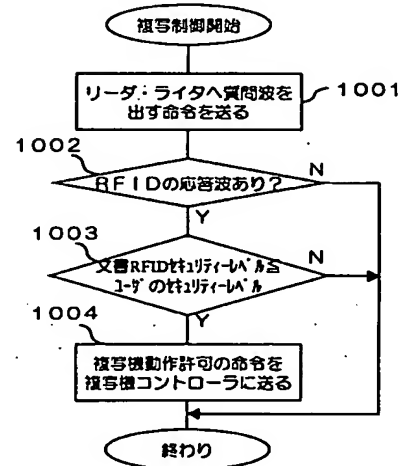
【図3】



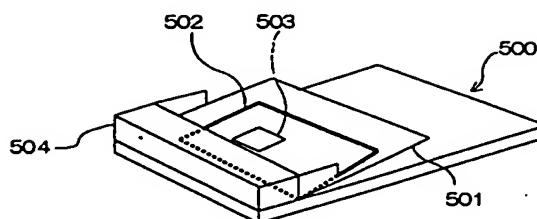
【図4】



【図5】



【図7】



【図6】

(a)

文書ID	許可ユーザID
D1	U1, U2, ...
D2	U1, U4, ...
...	...

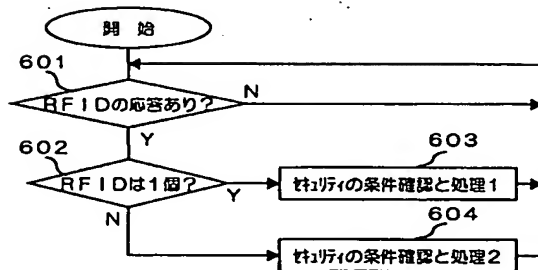
(b)

文書セキュリティレベル	許可ユーザID
レベル1	U1, U2, ...
レベル2	U2, U4, ...
...	...

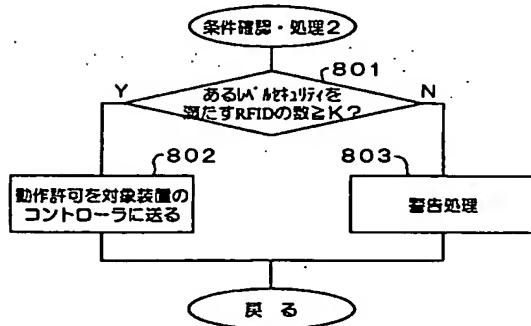
(c)

文書ID	許可ユーザセキュリティレベル
D1	レベル1以上
D2	レベル3以上
...	...

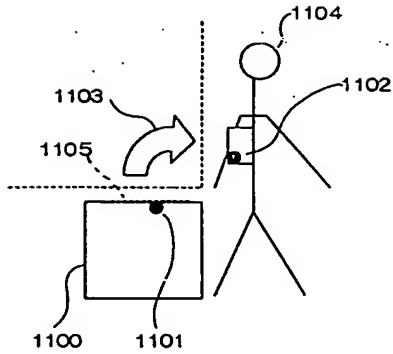
【図9】



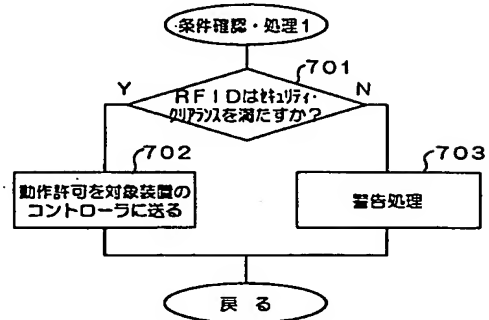
【図11】



【図8】



【図10】



【図12】

複写不可です。  
許可可能なカードをお持ちください。

## フロントページの続き

(51)Int.Cl. <sup>7</sup>	識別記号	F I	タームコード (参考)		
G 0 6 K	19/07	H 0 4 B	5/02	5 J 0 4 7	
	19/10	G 0 3 G	21/00	3 9 0	5 J 1 0 4
H 0 1 Q	1/12			5 5 4	5 K 0 1 2
H 0 4 B	5/02	G 0 6 K	19/00	H	9 A 0 0 1
H 0 4 L	9/32			R	
		H 0 4 L	9/00	6 7 3 A	
				6 7 3 E	

Fターム(参考) 2H027 EJ02 EJ04 GA23 GA30  
 2H034 BF08 FA01  
 5B017 AA05 AA06 BA05 BA06 BB03  
 BB06 CA16  
 5B035 AA14 BB09 BC00 CA23  
 5B058 CA15 KA31 YA13  
 5J047 AA07 AA08 AA09 AA17 AA19  
 BG06 EF05  
 5J104 AA07 KA01 NA05 NA35 NA36  
 NA41 NA42 PA14  
 5K012 AA03 AB03 AB04 AC06 BA02  
 BA07  
 9A001 CC05 HH34 JZ35 LL03